



**HOW TO IDENTIFY AND MITIGATE
FRAUD RISK IN MANUFACTURING**



“Manufacturing is significantly more likely than other industries to have experienced IP theft – 43% vs. 24% for all industries.”

- 2019 Global Fraud and Risk Report, Kroll

It is not uncommon for companies today to experience some form of misappropriation, corruption or fraud. However, the manufacturing sector, as a whole, seems to be more vulnerable to fraudulent activities than other industries.

According to [Kroll's 2019 Global Fraud and Risk Report](#) and [the Association of Certified Fraud Examiner's \(ACFE\) 2018 Report to the Nations](#), manufacturing had one of the highest reported cases of fraud of any sector:

- The **median loss** from fraud cases is **\$200,000 USD**
- In **47% of cases, employees were perpetrators** leading to a median loss of \$156,000 USD. When owners/executives were the perpetrators (23% of cases), the median loss was \$600,000 USD
- Manufacturing experiences the **highest incidence of leaks of internal information** (46% vs. 39% for all industries)
- Manufacturing reports **significant reputational damage** due to third-party relationships at a substantially higher rate than average (35% vs. 29% for all industries)
- Globally, 46% of manufacturers say that **leaks of internal information** significantly affected their organization in the last year, followed closely by IP theft at 43%
- 38% of Canadian manufacturers report that **adversarial social media activity** significantly affected their organization in the last year. **Fraud by external parties** was also cited as affecting 38%
- **Data theft** ranks as the highest risk priority for 69% of Canadian manufacturers compared to 87% of global manufacturers
- Looking ahead five years, manufacturers are most concerned about **large-scale coordinated cyberattacks (70%)** and a **significant financial crisis (69%)**



Instances of fraud are rampant in manufacturing because manufacturing environments present unique opportunities for employees, contractors, vendors, or cyber hackers alike, to take advantage of unsuspecting companies. This makes them vulnerable to significant financial loss and reputational risk.

There is often minimal oversight or lack of internal controls and proper automated systems within a manufacturing organization. This puts the business at risk to individuals who are willing to commit fraudulent activities, waste valuable resources, and abuse their authority.

From warehousing and distribution with possibilities of theft of raw materials and scrap parts, to financial and vendor statements or transactions with unusual or non-recurring events, there are numerous opportunities for “margin loss” or criminal activities to occur.

A lack of management understanding or support for automated systems, processes, and internal controls over procedures and protocols, is often what exposes these companies to the risk for loss of costly inventory, unauthorized transactions, altered financial or inventory records. All of which can all result in detrimental financial consequences and nonrecoverable reputational damage to their businesses.

Fraud is a serious, on-going problem affecting the manufacturing industry. Recognizing where manufacturing businesses may be at risk for possible fraudulent activity is a crucial part of the risk management process. This paper outlines how manufacturing leaders can be proactive in detecting and preventing fraudulent activities by:

- Understanding what constitutes as fraud
- Recognizing how fraud impacts manufacturers
- Detecting the “red flags” or indicators that point to fraud

COMMON FORMS OF FRAUD IN MANUFACTURING



The most common types of fraud in this sector include asset misappropriation, financial statement fraud, and corruption. Asset misappropriation involves the theft or misuse of the organization's cash and non-cash resources. Financial statement fraud can be defined as a scheme in which an employee intentionally causes a misstatement or omission of material information in the organization's financial reports. Corruption in manufacturing includes scenarios in which an employee misuses his or her influence in a business transaction in a way that violates his or her duty to the employer in order to gain a direct or indirect benefit.

Understanding the key vulnerabilities within the business and where fraudulent activities typically occur is the first step to mitigating risk in the organization.

COMMON FORMS OF FRAUD IN MANUFACTURING



1. Asset Misappropriation

Asset misappropriation accounted for 89 percent of the fraud cases reported in the 2019 Global Fraud and Risk Report.

What does this include?

- An organization's assets are taken through trickery or deceit
- Employee theft of inventory
- Falsification of records to obtain unauthorized cash (skimming, billing, expense reimbursement, payroll schemes)
- Larceny or misuse of equipment, inventory, supplies, cash, etc.

COMMON FORMS OF FRAUD IN MANUFACTURING



2. Financial Statements

While financial statement fraud only occurred in 10 percent of the fraud cases that occurred in the manufacturing industry, as outlined in the 2019 Global Fraud and Risk Report, this type of fraud tends to cause much higher losses than asset misappropriation.

What does this include?

- Prematurely recording revenue in the books prior to product being shipped to the customer
- Recording fictitious revenues or understating revenues
- Misappropriation of expenses
- Vendor, supplier, or procurement fraud for financial gain
- Larceny or misuse of equipment, inventory, supplies, cash, etc.

COMMON FORMS OF FRAUD IN MANUFACTURING



3. Corruption

Corruption was the most common scheme in every global region according to the 2019 Global Fraud and Risk Report.

What does this include?

- Inventory and product substitution/product counterfeiting
- Bribery in the form of invoice kickbacks or bid rigging
- Abuse of one's position or authority
- Purchase schemes where goods or services are overbilled by a vendor, in which an employee has an undisclosed ownership or financial interest
- Sales maneuvers where company goods are undersold by an employee to a company, in which the employee maintains a hidden interest

UNCOVERING FRAUD TO PREVENT LOSS



Manufacturing organizations should have a robust fraud risk management framework and on-going assessment strategy to help mitigate vulnerabilities. With more than half the victim organizations affected by fraud unable to recover losses, proactive measures to alleviate the risk fraud becomes even more critical. Manufacturing leaders and executive management should prioritize assessing and monitoring their organization's specific vulnerabilities and optimize a fraud prevention program.

The success of a fraud prevention initiative will improve if people feel that their wrongdoings will be detected. However, success is also reliant upon the actual mechanisms implemented and their ability to detect fraud. Ideally, the framework for business leaders should continuously improve the fraud risk management strategy—while regularly measuring the current and desired state of the business.

Preventing, detecting, and deterring fraud with fraud risk management techniques and forensic data analysis is highly recommended for manufacturing business leaders. Some preventive measures that can help detect instances of inventory fraud are regular counting cycles, robust inventory record-keeping, and rigorous stocking procedures supported with technologies such as Enterprises Resources Planning (ERP) solutions and processes such as bar code scanning, inventory identification, and inventory tracking.

UNCOVERING FRAUD TO PREVENT LOSS



Manufacturers can also prevent loss due to fraud by proactively using forensic data analysis to diagnose, detect, prevent, and respond to instances of fraud and corruption.

This can be achieved by performing periodic tests on high-risk transactions or areas of business that can identify and isolate suspicious financial or inventory transactions. Manufacturing companies need to proactively carry-out periodic analysis of relevant financial and inventory data to identify emerging issues as well as get to the root-cause faster, before the repercussions are detrimental to their bottom line.

While the risk of fraud can never be fully eliminated, manufacturing leaders should arm themselves with a proper understanding of fraud, as there are plenty of “red flags” or indicators to suggest opportunities or instances of fraud.

UNCOVERING FRAUD TO PREVENT LOSS



By looking for some of the following indicators, manufacturing leaders can uncover and mitigate fraud in their businesses.



1. Asset Misappropriation

What to look for?

- Inventory stored in unsecured or secluded warehouse areas
- Unusual after-hours or holiday access to plant/office
- Rarely sold or used products that are not physically verified on an on-going basis
- Increase in bad debt expenses
- Increase in inventory, as a percentage of total assets
- Reduction in inventory that cannot be accounted for
- Unusual expenses related to travel or maintenance of company assets
- Inability to support questionable costs for inventory
- Failure to reconcile inventories and financial records
- Inconsistent spending with budgeted spending levels
- Non-sequentially numbered POs or vendor orders

UNCOVERING FRAUD TO PREVENT LOSS



2. Financial Statements

What to look for?

- Accounting anomalies, such as growing revenue without a corresponding growth in cash flow
- Cash collections that fall below reported revenue
- Poor internal controls in the revenue collection process
- A sudden increase in “soft” expenses such as advertising or external consulting Multiple mailing addresses or P.O. boxes for a single vendor
- Frequent adjustments in Accounts Payables and/or Receivables records for returned goods
- Lack of control regarding posting to cash receipts and A/R sub-ledger activities Accumulation of cash due to infrequent deposits
- Voided transactions with no reasonable explanation

UNCOVERING FRAUD TO PREVENT LOSS



3. Corruption

What to look for?

- Employee acceptance of inappropriate gifts, travel, or entertainment
- An employee who makes accelerated payments to a particular vendor
- An employee who insists on using a certain vendor, or who makes excuses for deficiencies in a vendor's services
- A bidder or supplier who is not found online, or does not have a valid street address or business phone number
- Selecting a vendor who provides high-price, low-quality goods
- Deviations in communications between internal staff and suppliers, such as calls or text messages to mobile phones
- Transactions that are authorized by staff outside of business hours

CONCLUSION



Manufacturers must be proactive in identifying and managing fraud risks that can be an expensive and potentially devastating to a company's reputation. An environment with strong internal controls in place will help mitigate or reduce risk for manufacturing leaders. Implementing controls and procedures to measure risk can uncover areas of weakness with people, process, or technology that can be addressed.

Implementing a fraud risk management process does not need to be expensive or complicated. The cost of doing nothing can potentially cost you more.

ABOUT SYSPRO



SYSPRO is a global, independent provider of industry-built ERP software designed to simplify business complexity for manufacturers and distributors.

Focused on delivering optimized performance and complete business visibility, SYSPRO's strengths lie in a simplified approach to technology, expertise in a range of industries, and a commitment to future-proofing customer and partner success.



If you want to learn how SYSPRO can help mitigate and monitor fraud risks, visit [syspro.com](https://www.syspro.com).